Amendments to the Claims

Claim 1 (currently amended): A computer program product for efficiently generating pseudo-random bits, the computer program product embodied on one or more computer readable media and comprising:

computer-readable program code means for providing an input value comprising C random bits;

computer-readable program code means for generating an output sequence [[of]] comprising N pseudo-random bits using the provided C-bit input value as [[an]] a short exponent x of a 1-way function G**x mod P that comprises ~~comprising~~ modular exponentiation modulo a safe N-bit prime number P, wherein ~~a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and~~ a base G of the modular exponentiation is a fixed generator value;

computer-readable program code means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion; and

computer-readable program code means for using ~~C selected bits~~ the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the computer-readable program code means for generating while using ~~all N - C remaining bits~~ the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent"

assumption.

Claims 3 - 5 (canceled)

Claim 6 (currently amended): The computer program product according to Claim 1, wherein C = 160 ~~the length of the input value is 160 bits~~ and N = 1024, ~~a length of the safe prime number is 1024 bits.~~

Claim 7 (currently amended): The computer program product according to Claim 1, wherein C is greater than or equal to 160 and N is greater than or equal to 1024. ~~the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.~~

Claim 8 (canceled)

Claim 9 (currently amended): The computer program product according to Claim 1, wherein the (N-C)-bit portion is ~~N - C remaining bits are~~ concatenated to pseudo-random output bits previously generated by the computer-readable program code means for generating.

Claim 10 (currently amended): The computer program product according to Claim 1, wherein the (N-C)-bit portion is ~~N - C remaining bits are selected from the N bits of the generated output sequence as a~~ contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 11 (currently amended): The computer program product according to Claim 1, wherein the (N-C)-bit portion is ~~N - C remaining bits are selected from the N bits of the generated output sequence as~~ a non-contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 12 (previously presented): The computer program product according to Claim 1, further comprising computer-readable program code means for using the desired number of generated pseudo-random bits as input to an encryption operation.

Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a computing environment, comprising:

means for providing an input value comprising C random bits;

means for generating an output sequence [[of]] comprising N pseudo-random bits using the provided C-bit input value as [[an]] a short exponent x of a 1-way function G**x mod P that comprises ~~comprising~~ modular exponentiation modulo a safe N-bit prime number P, ~~wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and~~ a base G of the modular exponentiation is a fixed generator value;

means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion; and

means for using ~~C selected bits~~ the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the means for generating while using ~~all N - C remaining bits~~ the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.

Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 15 - 17 (canceled)

Claim 18 (currently amended): The system according to Claim 13, wherein ~~the length of the input value is 160 bits~~ C = 160 and ~~a length of the safe prime number is 1024 bits~~ N = 1024.

Claim 19 (currently amended): The system according to Claim 13, wherein ~~the length of the input value~~ C is at least 160 [[bits]] and ~~the length of the generated output sequence~~ N is at least 1024 [[bits]].

Claim 20 (canceled)

Claim 21 (currently amended): The system according to Claim 13, wherein the ~~N - C remaining bits are~~ (N-C)-bit portion is concatenated to pseudo-random output bits previously generated by the means for generating.

Claim 22 (currently amended): The system according to Claim 13, wherein the ~~N - C remaining bits are selected from the N bits of the generated output sequence as~~ (N-C)-bit portion is a contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 23 (currently amended): The system according to Claim 13, wherein the ~~N - C remaining bits are selected from the N bits of the generated output sequence as~~ (N-C)-bit portion is a non-contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 24 (previously presented): The system according to Claim 13, further comprising means for using the desired number of generated pseudo-random output bits as input to an encryption operation.

Claim 25 (currently amended): A programmatic method for efficiently generating pseudo-random bits, comprising the steps of:

providing an input value comprising C random bits;

generating an output sequence [[of]] comprising N pseudo-random bits using the provided C-bit input value as [[an]] a short exponent x of a 1-way function G**x mod P that comprises ~~comprising~~ modular exponentiation modulo a safe N-bit prime number P, ~~wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and~~ a base G of the modular exponentiation is a fixed generator value;

separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion; and

using ~~C selected bits~~ the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the generating step while using ~~all N - C remaining bits~~ the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits,

until a desired number of pseudo-random output bits have been generated.

Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 27 - 29 (canceled)

Claim 30 (currently amended): The method according to Claim 25, wherein ~~the length of the input value is at least~~ C = 160 [[bits]] and ~~a length of the safe prime number is at least~~ N = 1024 [[bits]].

Claim 31 (canceled)

Claim 32 (currently amended): The method according to Claim 25, wherein ~~the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits~~ C is greater than or equal to 160 and N is greater than or equal to 1024.

Claim 33 (canceled)

Claim 34 (currently amended): The method according to Claim 25, wherein the ~~N - C remaining bits are~~ (N-C)-bit portion is concatenated to pseudo-random output bits previously generated by the generating step.

Claim 35 (currently amended): The method according to Claim 25, wherein the ~~N - C remaining bits are~~ (N-C)-bit portion is ~~selected from the N bits of the generated output sequence as a~~ contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 36 (currently amended): The method according to Claim 25, wherein the ~~N - C remaining bits are~~ (N-C)-bit portion is ~~selected from the N bits of the generated output sequence as a~~ non-contiguous group of (N-C) bits from the generated N-bit output sequence.

Claim 37 (previously presented): The method according to Claim 25, further comprising the step of using the desired number of generated pseudo-random output bits as input to an encryption operation.

Claim 38 (canceled)

Claim 39 (currently amended): An encryption system, comprising:

means for providing an input value comprising C random bits;

means for generating an output sequence [[of]] comprising N pseudo-random bits using the provided C-bit input value as [[an]] a short exponent x of a 1-way function G**x mod P that comprises ~~comprising~~ modular exponentiation modulo a safe N-bit prime number P, wherein ~~a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and~~ a base G of the modular exponentiation is a fixed generator value;

means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion;

means for using ~~C selected bits~~ the C-bit portion of the generated N-bit output sequence as the provided input value for a next iteration of the means for generating while using ~~all N - C remaining bits~~ the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated; and

means for using the desired number of generated pseudo-random bits as input to an encryption operation.

Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 41 - 43 (canceled)

Claim 44 (currently amended): The encryption system according to Claim 39, ~~wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits~~ C = 160 and N = 1024.

Claims 45 - 46 (canceled)

Claim 47 (currently amended): The encryption system according to Claim 39, wherein the ~~N - C remaining bits are~~ (N-C)-bit portion is concatenated to pseudo-random output bits previously

generated by the means for generating.

Claim 48 (new): The computer program product according to Claim 1, wherein N is greater than or equal to (C * 6).

Claim 49 (new): The system according to Claim 13, wherein N is greater than or equal to (C * 6).

Claim 50 (new): The method according to Claim 25, wherein N is greater than or equal to (C * 6).

Claim 51 (new): The encryption system according to Claim 39, wherein N is greater than or equal to (C * 6).

Claim 52 (new): A programmatic method for efficiently generating pseudo-random bits, comprising the steps of:

providing an N-bit input value in which (N-C) uppermost contiguous ones of the bits are all set to zeroes and in which C lowermost contiguous ones of the bits are random;

generating an output sequence comprising N pseudo-random bits using the provided N-bit input value as an effectively-short, C-bit exponent x of a 1-way function G**x mod P that comprises modular exponentiation modulo a safe N-bit prime number P, wherein a base G of the modular exponentiation is a fixed generator value;

separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion;

creating a new N-bit input value in which the (N-C) uppermost contiguous ones of the bits are all set to zeroes and in which the lowermost C contiguous ones of the bits are set to the C-bit portion; and

using the new N-bit input value as the provided input value for a next iteration of the generating step while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated.